PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-051816
(43)Date of publication of application : 21.02.2003

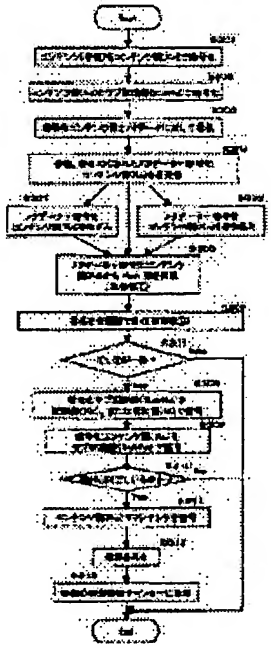
(51)Int.Cl. H04L 9/08
G06F 17/60
G09C 1/00
H04N 7/08
H04N 7/081
H04N 7/16
// H04N 7/167

(21)Application number : 2001-239148
(22)Date of filing : 07.08.2001

(71)Applicant : SONY CORP
(72)Inventor : SATO HIDEO
KATO ARIYOSHI

(54) CONTENTS DISTRIBUTION SYSTEM, CONTENTS DISTRIBUTION METHOD, DATA PROCESSOR, DATA PROCESSING METHOD, AND COMPUTER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a contents distribution system for distributing encrypted contents which can effectively exclude illegal use of contents.
SOLUTION: The system that distributes encrypted contents and allows only legal users to utilize the contents is configured such that a contents management distribution site for distributing contents generates a hash value of data incorporating meta data containing contents cost information and a contents key applied to contents encryption processing and executes an electronic signature, a user site receiving the data acquires the contents key stored in signature object data on the condition that signature verification is established, and the system can prevent illegal use of contents through falsification or replacement of the meta data.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－51816
（Ｐ2003－51816Ａ）
(43)公開日　平成15年２月21日(2003.2.21)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　17/60	３３２	５Ｃ０６３
Ｇ０６Ｆ　17/60	３３２	Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｃ０６４
Ｇ０９Ｃ　1/00	６４０		６４０Ｚ	５Ｊ１０４
		Ｈ０４Ｎ　7/16	Ｃ	
Ｈ０４Ｎ　7/08		Ｈ０４Ｌ　9/00	６０１Ｂ	

審査請求　未請求　請求項の数21　ＯＬ　（全 24 頁）　最終頁に続く

(21)出願番号　特願2001－239148(Ｐ2001－239148)

(22)出願日　平成13年８月７日(2001.8.7)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　佐藤　英雄
東京都品川区北品川６丁目７番35号　ソニー株式会社内

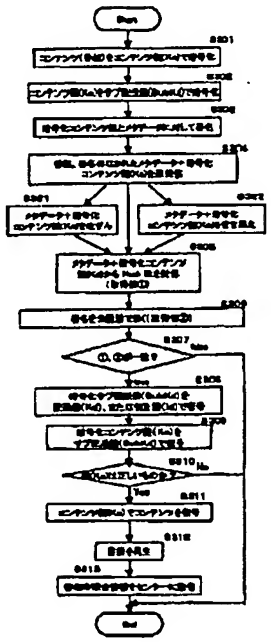
(72)発明者　加藤　有美
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】　暗号化コンテンツを配信するシステムにおいて、コンテンツの不正利用の効果的排除を可能としたコンテンツ配信システムを実現する。
【解決手段】　暗号化コンテンツの配信を行ない、正規ユーザにおいてのみコンテンツの利用を許容するシステムにおいて、コンテンツ配信を行なうコンテンツ管理配信サイトにおいて、コンテンツの価格情報を含むメタデータと、コンテンツの暗号処理に適用するコンテンツ鍵を併せたデータのハッシュ値を生成して電子署名を実行し、データを受信したユーザサイトにおいて、署名検証の成立を条件として署名対象データ中に格納されたコンテンツ鍵の取得を可能とする構成とし、メタデータ改竄、あるいは置き換えによるコンテンツ不正利用を防止可能とした。



【特許請求の範囲】
【請求項１】コンテンツ配信サイトから暗号化コンテンツを配信し、ユーザサイトにおいて暗号化コンテンツの復号処理を実行するコンテンツ配信システムにおいて、
前記コンテンツ配信サイトは、
コンテンツをコンテンツ鍵で暗号化した暗号化コンテンツと、前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとをユーザサイトに送信するとともに、前記暗号化コンテンツ鍵と前記メタデータとを含むデータのハッシュ値に対する電子署名をユーザサイトに送信する処理を実行する構成を有し、
前記ユーザサイトは、
前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行する構成を有することを特徴とするコンテンツ配信システム。
【請求項２】前記ユーザサイトは、
前記電子署名の検証処理として、
前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、
前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行する構成であり、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行する構成であることを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項３】前記メタデータは、コンテンツの利用価格情報を含み、
前記ユーザサイトは、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティテイに対して生成した課金情報を送信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項４】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、
前記コンテンツ配信サイトは、前記サブ配送鍵（ＳｕｂＫｄ）を配送鍵（Ｋｄ）で暗号化した鍵データをユーザサイトに送信する処理を実行する構成であり、
前記ユーザサイトは、
前記電子署名の検証成立を条件として、予め保有する前記配送鍵（Ｋｄ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項５】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、
前記コンテンツ配信サイトは、前記サブ配送鍵（ＳｕｂＫｄ）を、各ユーザサイトに個別に配布された個別鍵（Ｋｉ）で暗号化した鍵データをユーザサイトに送信する処理を実行する構成であり、
前記ユーザサイトは、
前記電子署名の検証成立を条件として、予め保有する前記個別鍵（Ｋｉ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項６】コンテンツ配信サイトから暗号化コンテンツを配信し、ユーザサイトにおいて暗号化コンテンツの復号処理を実行するコンテンツ配信方法であり、
前記コンテンツ配信サイトにおいて、
コンテンツをコンテンツ鍵で暗号化した暗号化コンテンツと、前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとをユーザサイトに送信するとともに、前記暗号化コンテンツ鍵と前記メタデータとを含むデータのハッシュ値に対する電子署名をユーザサイトに送信する処理を実行し、
前記ユーザサイトにおいて、
前記電子署名の検証処理を実行し、該電子署名検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行することを特徴とするコンテンツ配信方法。
【請求項７】前記ユーザサイトは、
前記電子署名の検証処理として、
前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、
前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行し、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行することを特徴とする請求項６に記載のコンテンツ配信方法。
【請求項８】前記メタデータは、コンテンツの利用価格情報を含み、
前記ユーザサイトは、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティテイに対して生成した課金情報を送信する処理を実行することを特徴とする請求項６に記載のコンテンツ配信方法。
【請求項９】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、
前記コンテンツ配信サイトは、前記サブ配送鍵（ＳｕｂＫｄ）を配送鍵（Ｋｄ）で暗号化した鍵データをユーザサイトに送信する処理を実行し、
前記ユーザサイトは、
前記電子署名の検証成立を条件として、予め保有する前記配送鍵（Ｋｄ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ

鍵を取得することを特徴とする請求項６に記載のコンテンツ配信方法。
【請求項１０】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、
前記コンテンツ配信サイトは、前記サブ配送鍵（ＳｕｂＫｄ）を、各ユーザサイトに個別に配布された個別鍵（Ｋｉ）で暗号化した鍵データをユーザサイトに送信する処理を実行し、
前記ユーザサイトは、
前記電子署名の検証成立を条件として、予め保有する前記個別鍵（Ｋｉ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする請求項６に記載のコンテンツ配信方法。
【請求項１１】暗号化コンテンツの復号処理を実行するデータ処理装置であり、
コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行し、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行するデータ処理手段を有することを特徴とするデータ処理装置。
【請求項１２】前記データ処理手段は、
前記電子署名の検証処理として、
前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、
前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行し、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行する構成を有することを特徴とする請求項１１に記載のデータ処理装置。
【請求項１３】前記データ処理装置は、
前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行する構成を有することを特徴とする請求項１１に記載のデータ処理装置。
【請求項１４】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、
前記データ処理装置は、
前記電子署名の検証成立を条件として、予め保有する配送鍵（Ｋｄ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする請求項１１に記載のデータ処理装置。
【請求項１５】前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、
前記データ処理装置は、
前記電子署名の検証成立を条件として、予め保有する個別鍵（Ｋｉ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする請求項１１に記載のデータ処理装置。
【請求項１６】暗号化コンテンツの復号処理を実行するデータ処理方法であり、
コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行し、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行することを特徴とするデータ処理方法。
【請求項１７】前記電子署名の検証処理は、
前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、
前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理であり、
該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行することを特徴とする請求項１６に記載のデータ処理方法。
【請求項１８】前記データ処理方法は、さらに、
前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行することを特徴とする請求項１６に記載のデータ処理方法。
【請求項１９】前記データ処理方法において、
前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、
前記電子署名の検証成立を条件として、予め保有する配送鍵（Ｋｄ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする請求項１６に記載のデータ処理方法。
【請求項２０】前記データ処理方法において、
前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、
前記電子署名の検証成立を条件として、予め保有する個別鍵（Ｋｉ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする請求項１６に記載のデータ処理方法。
【請求項２１】暗号化コンテンツの復号処理を含むデータ処理をコンピュータ・システム上で実行せしめるコン

ピュータ・プログラムであって、
コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行するステップと、
前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行するステップと、
を具備することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラムに関する。特に、暗号化されたコンテンツを配信するシステムにおいて、コンテンツの価格情報等を含むメタデータの改竄、置き換えなどによるコンテンツの不正利用を防止するコンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラムに関する。

【０００２】

【従来の技術】昨今、音楽データ、画像データ、ゲームプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット、衛星を介した通信他、有線、無線の各種通信網を介して配信するサービスが盛んになってきている。また、ＤＶＤ、ＣＤ、メモリカード等の流通可能な記憶媒体を介したコンテンツ流通も盛んになってきている。これらの流通コンテンツは、ユーザの所有する例えば、ＴＶ、ＰＣ（Personal Computer）、再生専用器、あるいはゲーム機器等において、再生、利用される。

【０００３】通信網を介して配信されるコンテンツは、例えば通信機能を有するセットトップボックスによって受信され、ＴＶ他の再生装置において再生可能なデータに変換されて再生される。あるいは通信インタフェースを備えたＴＶ、再生装置、ゲーム機器、ＰＣ等の情報機器によって受信されて再生される。

【０００４】ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウエアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【０００５】ユーザに対する利用制限を実現する１つの手法が、配布コンテンツの暗号化処理である。例えば著作権保証の要請されるコンテンツを衛星あるいはインターネット等を介して配信する場合にコンテンツを暗号化して配信し、正規ユーザに対してのみ復号鍵を配布する。正規ユーザは配布された復号鍵によって暗号化コンテンツの復号を実行し、コンテンツを再生する構成である。

【０００６】例えば、正規ユーザに対して暗号化コンテンツを復号するための鍵を格納したメモリ媒体（例えばＩＣカード）を配布し、ユーザは配布されたＩＣカードをセットトップボックスまたは受信機にセットし、セットしたカードの格納鍵を用いて暗号化コンテンツの復号処理を実行して再生する構成がある。

【０００７】図１を用いて、コンテンツをコンテンツ鍵で暗号化して配信するコンテンツ配信システム構成例について説明する。

【０００８】図１は、コンテンツ（番組）を制作または提供するコンテンツ提供サイト１０と、コンテンツを受信して再生するユーザサイト２０における処理を説明する図である。管理センター３０は、配送鍵（Ｋｄ：Distribution Key）をコンテンツ提供サイト１０とユーザサイト２０に提供する。ユーザサイト２０には、例えばデータの取り出しを防止したセキュアモジュールとしてのＩＣカード内に配送鍵（Ｋｄ）を格納して提供する。

【０００９】図１に示す番号（１）～に沿って処理が進行する。処理の詳細について説明する。まず、コンテンツ提供サイト１０では、（１）コンテンツを暗号化するためのコンテンツ鍵（Ｋｃ）を生成し、（２）生成したコンテンツ鍵（Ｋｃ）を用いてコンテンツの暗号化処理を実行する。暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、例えば代表的な共通鍵暗号アルゴリズムであるＤＥＳ（Data Encryption Standard）が適用できる。

【００１０】共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な暗号化方式がＤＥＳ（データ暗号標準：Data encryption standard）である。

【００１１】さらに、安全性を増すためにＤＥＳアルゴリズムを３重にして処理を行なうトリプルＤＥＳを適用してもよい。ＤＥＳ暗号化処理では鍵長５６ビットの鍵を生成してコンテンツ鍵として使用し、トリプルＤＥＳでは１１２ビットの鍵長を持つ鍵をコンテンツ鍵として生成する。このようなコンテンツ鍵は、乱数発生装置において発生した乱数に基づいて生成するものであり、コンテンツ毎に生成する。

【００１２】コンテンツ提供サイト１０は、生成したコンテンツ鍵（Ｋｃ）を用いてコンテンツを暗号化するとともに、（３）生成したコンテンツ鍵（Ｋｃ）を管理センター３０から受領した配送鍵（Ｋｄ）を用いて暗号化する。この場合の暗号化アルゴリズムもやはりＤＥＳや

トリプルＤＥＳなどの共通鍵アルゴリズムが用いられる。さらに暗号化コンテンツ鍵（Ｋｃ）にコンテンツの利用条件、すなわちコピーしてよいか、あるいは価格などの付加情報によって構成されるメタデータを付加する。さらに、コンテンツ提供サイト１０は、メタデータの改竄防止のためにメタデータのハッシュ（Ｈａｓｈ）値を算出し、ハッシュ値に対してコンテンツ提供サイト１０の秘密鍵を用いて電子署名を施す。

【００１３】コンテンツ提供サイト１０は、（４）コンテンツ鍵（Ｋｃ）で暗号化したコンテンツと、配送鍵（Ｋｄ）で暗号化したコンテンツ鍵（Ｋｃ）と、署名を施したメタデータ、さらに、コンテンツ提供サイト１０の公開鍵証明書をユーザに向けて配信する。これらのデータは共に衛星、インターネットなどの配信経路を通じてユーザサイト２０の受信機に送られ、例えば受信機内のＨＤＤなどの蓄積装置に蓄積される。

【００１４】ユーザサイト２０では、まず、（５）受信したメタデータに対する署名検証を行なう。まず、コンテンツ提供サイト１０の公開鍵証明書を、ユーザサイト２０に予め配布されている認証局の公開鍵で検証し、公開鍵証明書からコンテンツ提供サイト１０の公開鍵を取り出し、取り出したコンテンツ提供サイト１０の公開鍵によって署名検証を実行する。

【００１５】ユーザは、購入条件を確認して購入を決定すると、（６）管理センター３０から受領した配送鍵（Ｋｄ）を用いて暗号化コンテンツ鍵（Ｋｃ）の復号を行なう。配送鍵（Ｋｄ）は、前述したように正しい契約が行われた受信機または、受信機に装着されたカードモジュールなどの安全なモジュール内に格納されている。

【００１６】暗号化されたコンテンツ鍵が受信機内で配布鍵によって復号化されると、利用条件に基づき、（７）コンテンツ鍵を用いてコンテンツが復号されて再生される。さらに、再生と同時に課金ログを生成し、生成した課金ログをこの配信サービスを行うための管理センター３０に送信し決済を行う構成とすることができる。

【００１７】管理センター３０は配送鍵（Ｋｄ）の管理、ユーザサイト２０の受信機あるいはカードモジュールの管理、顧客管理を行う。管理センター３０とユーザサイト２０の受信機あるいはカードモジュールとは電話回線などの下回線を通じて、一定期間毎に通信を行い、相互認証を行って配送鍵（Ｋｄ）の配布処理、および課金ログの回収処理を行う。

【００１８】図１の構成のように、コンテンツの暗号化はコンテンツの配信事業者または番組制作者としてのコンテンツ提供サイト１０が行うのが一般的で、コンテンツ提供サイト１０の暗号化装置に管理センターが管理している配送鍵（Ｋｄ）を入力することでコンテンツ提供サイト１０が暗号化コンテンツ鍵を生成する。管理センター３０は、正規ユーザであるユーザサイト２０に対しても暗号化コンテンツ鍵を復号するための配送鍵（Ｋｄ）を提供する。このように、管理センター３０は配送鍵（Ｋｄ）の管理および提供によりコンテンツの配信管理、課金処理を行なっている。

【００１９】また、ＣＳあるいはＢＳ放送等、衛星を用いたコンテンツ配信においては、フラット課金、すなわち月極めの一定料金で有料番組が視聴できる形態としたサービスも存在する。この場合には、視聴が許された受信機あるいはカードモジュールに対応して各々異なる個別鍵を設定する。放送局は、設定したすべての個別鍵で暗号化コンテンツ鍵を暗号化してコンテンツと共に衛星から配布する。この構成の場合も、すべての個別鍵が管理センタから配信事業者あるいは番組制作者に渡され、コンテンツ鍵が暗号化される。このようなシステム具体例として、ＣＳあるいはＢＳデジタル放送で採用されているＣＡＳ（Conditional Access System）がある。

【００２０】ＣＡＳ（Conditional Access System）は、配信番組（コンテンツ）をスクランブル処理し、スクランブルを解くための鍵(スクランブル鍵：Ｋｓｃ)を番組とともに、番組付帯情報として送信する。正規ユーザには、ＩＣカードが予め配布される。ＩＣカードには、暗号化されたスクランブル鍵（Ｋｓｃ）を復号するためのワーク鍵（Ｋｗｋ）が格納される。

【００２１】ただしワーク鍵（Ｋｗｋ）を固定化すると、鍵の漏洩の可能性があるので、ワーク鍵（Ｋｗｋ）は定期的に更新する。更新時には更新されたワーク鍵（Ｋｗｋ）を暗号化して配信する。ユーザに対して送信するスクランブル鍵（Ｋｓｃ）は、コンテンツ番組情報を含むＥＣＭ（Entitlement Control Message）内に含ませて放送データとして送信する。また、ワーク鍵（Ｋｗｋ）は、各ユーザに渡されているＩＣカードの識別子（ＩＤ）を付加情報として持つＥＭＭ（Entitlement Management Message）に含ませて放送波で送信する。

【００２２】暗号化されたワーク鍵は、正規ユーザに配布されているＩＣカードに格納されたマスタ鍵（Ｋｍ）を用いることによって復号可能となる。ＩＣカードに格納されたマスタ鍵（Ｋｍ）は、各ＩＣカード毎に異なる固有の鍵（個別鍵）である。

【００２３】マスタ鍵（Ｋｍ）は各ＩＣカードに固有の鍵であるため、更新されたワーク鍵（Ｋｗｋ）を暗号化して配信する場合には、正規ユーザの受信機の数（＝マスタ鍵の数）に対応する数の暗号化ワーク鍵を配信する。配信する複数の暗号化ワーク鍵の各々にはＩＣカード各々に対応したＩＤ番号が付与されており、受信機側では、自己のＩＣカードに一致するＩＤを持つ暗号化ワーク鍵データを選択して、ＩＣカードに格納されたマスタ鍵（Ｋｍ）を適用した復号処理を実行してワーク鍵を取得する。

【００２４】ユーザは取得したワーク鍵（Ｋｗｋ）を用いてスクランブルコンテンツ（番組）とともに配信され

た暗号化スクランブル鍵（Ｋｓ）の復号処理を実行して、スクランブル鍵（Ｋｓ）を取得して、取得したスクランブル鍵（Ｋｓ）を用いてスクランブルコンテンツ（番組）のスクランブル解除（デスクランブル）処理を実行してコンテンツ（番組）を再生する。

【００２５】

【発明が解決しようとする課題】上記のようなコンテンツ配信システムにおいて、コンテンツの利用条件、すなわちコピーしてよいか、あるいは価格などの付加情報によって構成されるメタデータを暗号化コンテンツ鍵とともに送信する際、コンテンツ提供サイト１０は、メタデータの改竄防止のためにメタデータのハッシュ（Ｈａｓｈ）値を算出し、ハッシュ値に対してコンテンツ提供サイト１０の秘密鍵を用いて電子署名を施していた。

【００２６】ユーザサイトでは、受信したメタデータから計算したハッシュ（Ｈａｓｈ）値と、署名を公開鍵を適用した復号処理により解いて取得される復号値としてのハッシュ（Ｈａｓｈ）値を比較して、一致したら改竄なしと判定し、利用条件を確認した後、配送鍵（Ｋｄ）やワーク鍵（Ｋｗ）を適用した復号処理を実行可能としてコンテンツ鍵の取り出し、コンテンツを利用していた。

【００２７】しかし、従来の構成では、あるコンテンツに対応した価格情報を設定しているメタデータを他のコンテンツに対応付けるなどの処理により、例えば、値段の高い番組情報と、値段の安い番組情報のすりかえを行ない、安い値段のコンテンツに対応するメタデータを高い番組の再生に利用するなどの不正が発生する可能性があった。

【００２８】従来のメタデータの署名検証処理、コンテンツ利用について図２を用いて説明する。コンテンツ提供サイト（センター）は番組Ａをコンテンツ鍵（Ｋｃ－ａ）で暗号化し、番組Ａの価格情報を含むメタデータのハッシュ値をコンテンツ提供サイトの秘密鍵（Ｋｓ）による暗号化処理で署名を生成し、これらをユーザサイトに送信する。ユーザサイト側は、コンテンツ提供サイト（センター）の秘密鍵（Ｋｓ）に対応する公開鍵を公開鍵証明書から取り出して、公開鍵を適用して署名を解いて取得した値と、メタデータから計算したハッシュ（Ｈａｓｈ）値とが一致しているかどうかのチェックを行う。一致していれば、購入条件等のメタデータが改ざんされていないものとして、上述の配送鍵または個別鍵等の鍵（Ｋｗ）で暗号化コンテンツ鍵（Ｋｃ－ａ）を復号してコンテンツ鍵（ｋｃ－ａ）を取得し、取得したコンテンツ鍵（Ｋｃ－ａ）を使用して番組Ａを再生することが可能となる。番組Ｂについても、全く同様の処理により、コンテンツ鍵（ｋｃ－ｂ）を取得し、取得したコンテンツ鍵（Ｋｃ－ｂ）を使用して番組Ｂの再生が可能となる。

【００２９】一方、メタデータの改竄、置き換えによる不正なコンテンツ利用例について図３を参照して説明する。図３（ａ）に示すように、例えば３００円の番組Ａを１００円で見ようと、メタデータを改竄した場合。改竄したメタデータからハッシュ（Ｈａｓｈ）値を計算したものは、コンテンツ提供サイト（センター）から送られてきたハッシュ（Ｈａｓｈ）値と異なる。両者が一致しないので、再生することは不可能である。

【００３０】しかし、図３（ｂ）に示すように、例えば１０００円の番組Ｂを見るために、３００円の番組Ａのメタデータと署名を不正に利用する。まず、ユーザは、３００円の番組Ａのメタデータについての署名検証を１０００円の番組Ｂに対応する処理として実行する。この場合、番組Ａのメタデータからハッシュ（Ｈａｓｈ）値を計算したものと、番組Ａを購入した際にコンテンツ提供サイト（センター）から送られてきた番組Ａのハッシュ（Ｈａｓｈ）値は、本来番組Ｂのものではないが、番組Ｂのものとして両方とも番組Ａから置き換えられたものなので、一致してしまう。一致したことが証明されれば、そこでシステムは、次のステップの処理への移行を許可してしまう。次ステップでは、配送鍵または個別鍵等の固有の鍵（Ｋｗ）で暗号化コンテンツ鍵（Ｋｃ－ｂ）を復号してコンテンツ鍵（ｋｃ－ｂ）を取得し、取得したコンテンツ鍵（Ｋｃ－ｂ）を使用して番組Ｂを再生することが可能となる。その際、管理センターに送られる課金情報は置きかえられたメタ情報である番組Ａの３００円になってしまう。

【００３１】従来のシステムにおける署名検証処理に基づくコンテンツ（番組）再生処理との対応について図４を用いて説明する。ユーザサイトの例えばセットトップボックス等のシステムでは、メタデータからハッシュ（Ｈａｓｈ）値を計算し、また、コンテンツ提供サイト（センター）の秘密鍵（Ｋｓ）に対応する公開鍵を公開鍵証明書から取り出して、署名をコンテンツ提供サイトの公開鍵で解いて得たハッシュ（Ｈａｓｈ）値との比較を実行する。この比較において一致と判定されると、購入条件等のメタデータが改ざんされていないものと判断され、次の処理ステップへの移行が許可される。

【００３２】署名検証成功によって実行可能となる処理ステップは、配送鍵または個別鍵等の固有の鍵（Ｋｗ）で暗号化コンテンツ鍵（Ｋｃ）を復号してコンテンツ鍵（ｋｃ）を取得し、取得したコンテンツ鍵（Ｋｃ）を使用して番組を再生する処理である。メタデータが番組Ａに対応するものであれば、番組Ａのコンテンツ鍵（Ｋｃ－ａ）の取得および番組Ａの再生は、正当利用であるが、メタデータが番組Ａに対応するにもかかわらず、ハッシュ値の一致を条件として番組Ｂのコンテンツ鍵（Ｋｃ－ｂ）の取得および番組Ｂの再生を可能とする処理も可能であり、不正なコンテンツ利用が行われる恐れがある。

【００３３】図５に、メタデータの置き換えによりコン

テンツの不正利用を行なう場合の手順を説明するフローを示す。各ステップについて説明する。ステップＳ１０１で、コンテンツ提供サイト（センター）は番組Ｂを、コンテンツ鍵（Ｋｃ）で暗号化し、ステップＳ１０２で、番組Ｂのメタデータ、センターの秘密鍵（Ｋｓ）で暗号化された署名と共にユーザサイトに対して送信する。

【００３４】ユーザサイトでは、送信されてきた番組Ｂを再生するために、ステップＳ１０３で、番組Ｂのメタデータと送信された署名を番組Ａのメタデータと送信された署名に置き換える。ステップＳ１０４で置き換えられた番組Ａのメタデータからハッシュ（Ｈａｓｈ）値を計算する（取得値を[illegible]とする）。次にステップＳ１０５で、署名部分（こちらも置き換えられた番組Ａの署名）をセンターの公開鍵で解く（取得値を[illegible]とする）。ステップＳ１０６で、[illegible]と[illegible]が一致しているかどうかの判断を行う。この場合、両方とも置き換えられたものなので、一致する。一致したことが証明されれば、そこで再生許可が出てしまうので、ステップＳ１０７で、番組Ｂが再生可能となってしまう。そして、番組Ｂを再生したにもかかわらず、ステップＳ１０８で、番組Ａの課金情報が管理センターに送られる。

【００３５】次に、ユーザサイト側のシステム、例えばセットトップボックス、再生装置等で実行されるハッシュ（Ｈａｓｈ）値の照合処理の手順について図６のフローチャートを用いて説明する。ステップＳ２０１で、メタデータからハッシュ（Ｈａｓｈ）値を計算する（取得値を[illegible]とする）。ステップＳ２０２で、送信されてきた署名を、公開鍵証明書から取り出した公開鍵を適用して解く（取得値を[illegible]とする）。ステップＳ２０３で、各取得値[illegible]と[illegible]が一致しているかどうかの判断を行う。一致していたら、ステップＳ２０４で、番組Ａに対応する暗号化コンテンツ鍵を配送鍵（Ｋｄ）または個別鍵（Ｋｗ）を適用した復号処理により、コンテンツ鍵（Ｋｃ）を取得する。ステップＳ２０５で、取得したコンテンツ鍵（Ｋｃ）で番組Ａを再生することが可能となる。さらに、ステップＳ２０６で、メタ情報に記録された課金情報がセンターに送られる。

【００３６】このように、従来のコンテンツ配信システムでは、コンテンツの利用条件、価格などの付加情報によって構成されるメタデータを送信する際、メタデータについてのハッシュ値生成、署名処理を実行し、ユーザサイトでは、受信した署名の検証成立により、コンテンツ鍵の取得ステップを実行する構成であり、署名検証対象のメタデータと、復号処理対象となる暗号化コンテンツ鍵との関連付けがなされていないため、あるコンテンツに対応しているメタデータについての署名検証に基づいて他のコンテンツに対応したコンテンツ鍵の取得処理を実行して不正にコンテンツを再生、利用するという事態が発生していた。

【００３７】本発明は、上述の問題点に鑑みてなされたものであり、署名検証処理を実行した正当な対応コンテンツをのみ利用可能な構成を実現し、不正なコンテンツ利用を排除可能としたコンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【００３８】

【課題を解決するための手段】本発明の第１の側面は、コンテンツ配信サイトから暗号化コンテンツを配信し、ユーザサイトにおいて暗号化コンテンツの復号処理を実行するコンテンツ配信システムにおいて、前記コンテンツ配信サイトは、コンテンツをコンテンツ鍵で暗号化した暗号化コンテンツと、前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとをユーザサイトに送信するとともに、前記暗号化コンテンツ鍵と前記メタデータとを含むデータのハッシュ値に対する電子署名をユーザサイトに送信する処理を実行する構成を有し、前記ユーザサイトは、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行する構成を有することを特徴とするコンテンツ配信システムにある。

【００３９】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザサイトは、前記電子署名の検証処理として、前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行する構成であり、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行する構成であることを特徴とする。

【００４０】さらに、本発明のコンテンツ配信システムの一実施態様において、前記メタデータは、コンテンツの利用価格情報を含み、前記ユーザサイトは、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティテイに対して生成した課金情報を送信する処理を実行する構成を有することを特徴とする。

【００４１】さらに、本発明のコンテンツ配信システムの一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、前記コンテンツ配信サイトは、前記サブ配送鍵（ＳｕｂＫｄ）を配送鍵（Ｋｄ）で暗号化した鍵データをユーザサイトに送信する処理を実行する構成であり、前記ユーザサイトは、前記電子署名の検証成立を条件として、予め保有する前記配送鍵（Ｋｄ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする。

【００４２】さらに、本発明のコンテンツ配信システム

の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、前記コンテンツ配信サイトは、前記サブ配送鍵（ＳｕｂＫｄ）を、各ユーザサイトに個別に配布された個別鍵（Ｋｉ）で暗号化した鍵データをユーザサイトに送信する処理を実行する構成であり、前記ユーザサイトは、前記電子署名の検証成立を条件として、予め保有する前記個別鍵（Ｋｉ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする。

【００４３】さらに、本発明の第２の側面は、コンテンツ配信サイトから暗号化コンテンツを配信し、ユーザサイトにおいて暗号化コンテンツの復号処理を実行するコンテンツ配信方法であり、前記コンテンツ配信サイトにおいて、コンテンツをコンテンツ鍵で暗号化した暗号化コンテンツと、前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとをユーザサイトに送信するとともに、前記暗号化コンテンツ鍵と前記メタデータとを含むデータのハッシュ値に対する電子署名をユーザサイトに送信する処理を実行し、前記ユーザサイトにおいて、前記電子署名の検証処理を実行し、該電子署名検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行することを特徴とするコンテンツ配信方法にある。

【００４４】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザサイトは、前記電子署名の検証処理として、前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行し、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行することを特徴とする。

【００４５】さらに、本発明のコンテンツ配信方法の一実施態様において、前記メタデータは、コンテンツの利用価格情報を含み、前記ユーザサイトは、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行することを特徴とする。

【００４６】さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、前記コンテンツ配信サイトは、前記サブ配送鍵（ＳｕｂＫｄ）を配送鍵（Ｋｄ）で暗号化した鍵データをユーザサイトに送信する処理を実行し、前記ユーザサイトは、前記電子署名の検証成立を条件として、予め保有する前記配送鍵（Ｋｄ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする。

【００４７】さらに、本発明のコンテンツ配信方法の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、前記コンテンツ配信サイトは、前記サブ配送鍵（ＳｕｂＫｄ）を、各ユーザサイトに個別に配布された個別鍵（Ｋｉ）で暗号化した鍵データをユーザサイトに送信する処理を実行し、前記ユーザサイトは、前記電子署名の検証成立を条件として、予め保有する前記個別鍵（Ｋｉ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする。

【００４８】さらに、本発明の第３の側面は、暗号化コンテンツの復号処理を実行するデータ処理装置であり、コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行し、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行するデータ処理手段を有することを特徴とするデータ処理装置にある。

【００４９】さらに、本発明のデータ処理装置の一実施態様において、前記データ処理手段は、前記電子署名の検証処理として、前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理を実行し、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行する構成を有することを特徴とする。

【００５０】さらに、本発明のデータ処理装置の一実施態様において、前記データ処理装置は、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティティに対して生成した課金情報を送信する処理を実行する構成を有することを特徴とする。

【００５１】さらに、本発明のデータ処理装置の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、前記データ処理装置は、前記電子署名の検証成立を条件として、予め保有する配送鍵（Ｋｄ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする。

【００５２】さらに、本発明のデータ処理装置の一実施態様において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、前記データ処理装置は、前記電子署名の検証成立を条件として、予め保有する個別鍵（Ｋｉ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵

（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得する構成であることを特徴とする。

【００５３】さらに、本発明の第４の側面は、暗号化コンテンツの復号処理を実行するデータ処理方法であり、コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行し、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行することを特徴とするデータ処理方法にある。

【００５４】さらに、本発明のデータ処理方法の一実施態様において、前記電子署名の検証処理は、前記コンテンツ配信サイトから受信した前記暗号化コンテンツ鍵と前記メタデータとを含むデータから算出したハッシュ値と、前記コンテンツ配信サイトの公開鍵を適用した前記署名の復号値との比較処理であり、該比較処理において両値の一致を条件として、前記暗号化コンテンツ鍵の取得処理を実行することを特徴とする。

【００５５】さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法は、さらに、前記メタ情報内の価格情報に基づく課金情報を生成して課金処理実行エンティテイに対して生成した課金情報を送信する処理を実行することを特徴とする。

【００５６】さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、前記電子署名の検証成立を条件として、予め保有する配送鍵（Ｋｄ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする。

【００５７】さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において、前記コンテンツ鍵の暗号化鍵は、サブ配送鍵（ＳｕｂＫｄ）であり、前記電子署名の検証成立を条件として、予め保有する個別鍵（Ｋｉ）を用いた復号処理により、前記サブ配送鍵（ＳｕｂＫｄ）の取得処理を実行し、前記サブ配送鍵（ＳｕｂＫｄ）を用いた復号処理により、コンテンツ鍵を取得することを特徴とする。

【００５８】さらに、本発明の第５の側面は、暗号化コンテンツの復号処理を含むデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、コンテンツの暗号処理用のコンテンツ鍵を暗号化した暗号化コンテンツ鍵と、コンテンツの利用条件を含むメタデータとを含むデータのハッシュ値に対する電子署名の検証処理を実行するステップと、前記電子署名の検証成立を条件として、前記署名対象データ中に含まれる前記暗号化コンテンツ鍵の取得処理を実行するステップと、を具備することを特徴とするコンピュータ・プログラムにある。

【００５９】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００６０】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００６１】

【発明の実施の形態】【システム概要】図７に本発明のコンテンツ配信システムを実現するシステム構成例を示す。図７において、コンテンツは、コンテンツ配信管理サイト２００のコンテンツ配信部（例えば放送局）２３０において暗号化（スクランブル処理も含む）されてコンテンツ配信部２３０から通信衛星、インターネット等の各種通信手段を介してユーザサイト１００の受信手段（例えばＳＴＢ：セットトップボックス）１２０に向けて配信される。

【００６２】ユーザサイト１００の受信手段１２０は、コンテンツ配信部２３０からの配信データを受信する通信インタフェースを備える。配信データ中のコンテンツは暗号化されており、所定の鍵を用いた復号処理を実行した後、ＴＶ等の出力手段１４０において出力される。コンテンツデータの復号処理等を実行するのは、データ処理手段１１０である。データ処理手段１１０と受信装置１２０間は例えばＩＥＥＥ１３９４インタフェースによって接続される。

【００６３】データ処理手段１１０は、受信コンテンツの蓄積用記憶装置として例えばＨＤＤを有し、さらにコンテンツの復号処理などを実行する暗号処理部としてのセキュアモジュール１１５を有する。セキュアモジュール１１５は、署名検証処理、暗号化コンテンツの復号処理を実行する暗号処理機能を持ち、暗号処理に適用する鍵の格納領域を有する。さらに、サービス管理センタ３００からの鍵配信処理の際の相互認証処理を実行する。

【００６４】コンテンツ配信部２３０によって配信されるコンテンツは、コンテンツ管理部２２０からコンテンツ配信部２３０に提供される。コンテンツ管理部２２０は各種のコンテンツプロバイダからコンテンツを受領して、価格情報、コピー制限等の付帯情報（メタ情報）を付加し、所定の暗号化処理、署名処理を実行して、コンテンツ配信部２３０に提供する。

【００６５】サービス管理センタ３００は、コンテンツの暗号処理鍵の鍵管理センタとしての機能を有する。さらに、ユーザサイト１００におけるコンテンツ利用状況に応じてセキュアモジュール１１５がメタ情報に基づいて生成する課金ログを収集する処理も実行する。セキュアモジュール１１５を持つユーザはサービス管理センタ３００との間で、コンテンツ利用に応じた料金についてサービス管理センタ３００が指定決済機関により決済処理を行なう旨の契約を結んでいる。また、サービス管理センタ３００は、必要に応じて、更新された鍵をユーザサイト１００のデータ処理手段１１０に送信する。

【００６６】なお、サービス管理センタ３００とユーザサイト１００のデータ処理手段１１０との間のデータ通信の際には相互認証処理が実行され、相互認証の成立を条件として各種のデータが相互認証において生成したセッション鍵で暗号化されて送受信される。相互認証は例えば公開鍵暗号方式を適用して実行される。公開鍵暗号方式の認証時に用いられる公開鍵証明書は認証局４００によって発行される。セキュアモジュール１１５には、公開鍵、秘密鍵の鍵ペア、認証局４００によって発行された公開鍵証明書等が格納される。認証局４００は、サービス管理センタ３００．コンテンツ管理配信サイト２００に対しても公開鍵証明書を発行する。

【００６７】データ処理手段１１０の構成を図８に示す。データ処理手段１１０は、セットトップボックス等の受信手段からの入力データについての署名検証処理、各種鍵、コンテンツの復号処理を実行する。また、サービス管理センタとの通信を実行して、コンテンツ復号に適用する鍵を受領し、コンテンツ利用時に生成するコンテンツ利用情報を記録した課金ログをサービス管理センタに送信する処理等を実行する。サービス管理センタは、課金ログに基づいて予めユーザとの契約において設定された決済機関からコンテンツ利用料金の決済処理を行なう。

【００６８】図８に示すデータ処理手段１１０の構成中、ＣＰＵ(Central processing Unit)１０１は、データ処理手段内で実行されるプログラムの実行制御を行ない、ＲＡＭ，ＲＯＭ等のデータ記憶手段、およびセキュアモジュール１１５として構成された暗号処理部間のデータ転送制御、通信Ｉ／Ｆ１０５，１０６を介したデータ転送制御処理を実行する。

【００６９】ＲＯＭ（Read-Only-Memory）１０２は、例えばＣＰＵ１０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（RandomAccess Memory）１０３は、ＣＰＵ１０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【００７０】ＨＤＤ１０４はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。

【００７１】セキュアモジール１１５、いわゆるＳＡＭ（Secure Application Module）によって構成される暗号処理部は、例えば外部から入力される暗号化コンテンツデータの復号処理、サービス管理センタからの鍵送信の際、あるいはログ情報のサービス管理センタに対する送信時の認証処理、暗号処理、署名検証等のデータの検証処理等を実行する。暗号／復号化部１２２は、これらの各種処理におけるデータの暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを実行する。内部メモリ１２３には、例えばセキュアモジュールに固有の識別子（ＩＤ）、暗号鍵等が格納される。制御部１２１は、セキュアモジュール１１５内の処理の制御、該部とのデータ転送制御等を実行する。

【００７２】通信インタフェース（Ｉ／Ｆ）１０５は、セットトップボックス、受信器、ＴＶ、再生装置等、コンテンツを受信する装置、あるいはコンテンツを再生する装置に接続するインタフェースであり、例えばＩＥＥＥ１３９４インタフェース機能を持つ。また、通信インタフェース（Ｉ／Ｆ）１０６は、サービス管理センタとの通信接続インタフェースであり、例えばインターネット接続インタフェーズであり、鍵の送受信、課金ログの送信等に利用される。

【００７３】［コンテンツ配信処理例１］コンテンツ配信処理例の詳細を図９を参照して説明する。本実施例に示すコンテンツ配信システムでは、配送鍵（Ｋｄ）およびサブ配送鍵（ＳｕｂＫｄ）を用いる。

【００７４】図９においては、Ａ．サービス管理センタ３００における処理（ａ１），（ａ２）、Ｂ．コンテンツ管理配信サイトにおける処理（ｂ１）～（ｂ５）、Ｃ．ユーザサイトにおける処理（ｃ１）～（ｃ４）を示している。各処理について、処理シーケンスに従って説明する。

【００７５】まず、Ａ．サービス管理センタ３００は、配送鍵（Ｋｄ）５０１およびサブ配送鍵（ＳｕｂＫｄ）５０２を生成し、これらについての処理を実行する。サービス管理センタ３００は、これらの鍵を乱数に基づいて生成する。サービス管理センタ３００は、（ａ１）の処理として、サブ配送鍵（ＳｕｂＫｄ）５０２を、配送鍵（Ｋｄ）５０１で暗号化する処理を行なう。

【００７６】暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、例えば代表的な共通鍵暗号アルゴリズムであるＤＥＳ（Data Encryption Standard）が適用できる。さらに、安全性を増すためにＤＥＳアルゴリズムを３重にして処理を行なうトリプルＤＥＳを適用してもよい。ＤＥＳ暗号化処理では鍵長５６ビットの鍵を適用し、トリプルＤＥＳでは１１２ビットの鍵長を持つ鍵を適用することになる。サービス管理センタ３００は、適用する暗号化方式に応じた鍵長の配送鍵（Ｋｄ）５０１およびサブ配送鍵（ＳｕｂＫｄ）５０２

を生成する。

【００７７】（ａ１）の処理の結果、配送鍵（Ｋｄ）で暗号化処理されたサブ配送鍵（ＳｕｂＫｄ）、すなわち、Ｅｎｃ［Ｋｄ（ＳｕｂＫｄ）］が生成される。ここでＥｎｃ［ａ（ｂ）］は、ｂをａで暗号化したデータを示すものとする。暗号化サブ配送鍵Ｅｎｃ［Ｋｄ（ＳｕｂＫｄ）］は、コンテンツ管理配信サイト２００に転送される。

【００７８】また、配送鍵（Ｋｄ）５０１についても、コンテンツ管理配信サイト２００に転送するが、通信路におけるデータ漏洩等の問題の発生を避けるため、（ａ２）の処理として、配送鍵（Ｋｄ）５０１の暗号化処理（ＤＥＳ）を実行してコンテンツ管理配信サイト２００に転送する。この場合の暗号化鍵としては、例えばコンテンツ管理配信サイト２００と、サービス管理センタ３００間において相互認証処理を実行し、認証処理の際に生成するセッション鍵（Ｋｓ）を適用することができる。あるいは双方が共通に保有する共通鍵、またはパスワードを用いて暗号化、復号化処理を実行する構成としてもよい。

【００７９】サービス管理センタ３００は、さらに、配送鍵（Ｋｄ）５０１をコンテンツ利用ユーザとして契約したユーザサイト１００に送付する。なお、この場合の鍵送付処理に際しては、コンテンツ管理配信サイト２００と、ユーザサイト１００のデータ処理手段間において相互認証処理を実行し、認証の成立を条件とし、認証処理の際に生成するセッション鍵を適用して配送鍵（Ｋｄ）を暗号化して送信することが好ましい。

【００８０】次に、Ｂ．コンテンツ管理配信サイト２００における処理について説明する。コンテンツ管理配信サイト２００は、まず（ｂ１）の処理として、コンテンツを暗号化するためのコンテンツ鍵（Ｋｃ）５０３を生成する。コンテンツ鍵は、乱数発生装置において発生した乱数に基づいて生成するものであり、コンテンツ毎に生成する。コンテンツ鍵による暗号化処理が例えばＤＥＳ暗号化処理である場合は鍵長５６ビットの鍵を生成してコンテンツ鍵とし、トリプルＤＥＳの場合は１１２ビットの鍵長を持つ鍵をコンテンツ鍵として生成する。

【００８１】次に、コンテンツ管理配信サイト２００は、（ｂ２）の処理として、生成したコンテンツ鍵（Ｋｃ）を用いてコンテンツの暗号化処理を実行する。暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、ＤＥＳ（Data Encryption Standard）、またはトリプルＤＥＳが適用できる。この暗号化処理の結果、暗号化コンテンツ：Ｅｎｃ［Ｋｃ（Ｃｏｎｔｅｎｔ）］５１１が生成される。

【００８２】さらに、コンテンツ管理配信サイト２００は、（ｂ３）の処理として、サービス管理センタ３００から受信した暗号化されたサブ配送鍵データ：Ｅｎｃ［Ｋｓ（ＳｕｂＫｄ）］をセッション鍵Ｋｓで復号し、サブ配送鍵（ＳｕｂＫｄ）５０２を取得する。

【００８３】次に、コンテンツ管理配信サイト２００は、（ｂ４）の処理として、取得したサブ配送鍵（ＳｕｂＫｄ）５０２を用いて、コンテンツ鍵（Ｋｓ）の暗号化処理を実行して暗号化コンテンツ鍵データ：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］５１２を生成する。

【００８４】次に、コンテンツ管理配信サイト２００は、暗号化コンテンツ鍵データ：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］５１２と、価格情報、コピー制限情報等の各種のコンテンツ関連利用情報からなるメタデータ５２１との双方のデータ、すなわち、（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）からハッシュ（Ｈａｓｈ）値を計算し、コンテンツ管理配信サイト２００の秘密鍵（Ｋｓ）を用いた署名生成処理（ｂ５）を実行する。署名生成処理は、例えば楕円曲線暗号方式の署名アルゴリズムであるＥＣＣ－ＤＳＡに従って実行される。

【００８５】コンテンツ管理配信サイト２００は、上述の処理によって生成した暗号化コンテンツ：Ｅｎｃ［Ｋｃ（Ｃｏｎｔｅｎｔ）］５１１、署名処理を施した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］５１２とメタデータ５２１、および、サービス管理センタ３００から受信した暗号化サブ配送鍵：Ｅｎｃ［Ｋｄ（ＳｕｂＫｄ）］５１３、さらに、コンテンツ管理配信サイト２００の公開鍵（Ｋｐ）を格納した公開鍵証明書をユーザサイトに向けて配信する。

【００８６】次に、上記各データを受信するユーザサイト１００における処理について説明する。ユーザサイト１００では、通信衛星またはインターネット等の通信手段を介して例えばセットトップボックス等の受信手段１２０においてデータ受信を行ない、受信データをデータ処理手段１１０に転送する。受信データは、データ処理手段１１０の例えばハードディスク等の記憶手段に一旦格納される。

【００８７】図９では、これらの格納データに対する処理手順を（ｃ１）～（ｃ４）として示している。まず、ユーザサイト１００では、（ｃ１）の処理として、コンテンツ管理配信サイト２００から受信した署名処理を施した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］５１２とメタデータ５２１の署名検証処理を実行する。署名検証処理は、署名を、受信した公開鍵証明書から取り出したコンテンツ管理配信サイト２００の公開鍵により解いた復号値と、受信データである（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）からハッシュ（Ｈａｓｈ）値を計算した結果とが一致するか否かによって実行される。一致していた場合は、署名が正しく、データ、すなわち、受信データである（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）の改竄がないと判定され、次の処理ステップの実行が許可される。署名検証において両データが一致しなかった場合は、データ改竄の可能性があると判定されて、次の処理が実行されず、処

理は終了する。

【００８８】署名検証に成功すると、次に、ユーザサイト１００では、（ｃ２）の処理として、コンテンツ管理配信サイト２００から受信した暗号化サブ配送鍵：Ｅｎｃ［Ｋｄ（ＳｕｂＫｄ）］５１３を、サービス管理センタ３００から受信した配送鍵（Ｋｄ）５０１を用いて復号処理を実行し、サブ配送鍵（ＳｕｂＫｄ）５０２を取得する。

【００８９】次に、ユーザサイト１００では、（ｃ３）の処理として、コンテンツ管理配信サイト２００から受信した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］５１２を、先の（ｃ１）の処理で取得したサブ配送鍵（ＳｕｂＫｄ）５０２を用いて復号処理を実行し、コンテンツ鍵（Ｋｃ）５０３を取得する。この復号処理の実行対象は、署名対象データ中に格納された暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］５１２である。

【００９０】次に、ユーザサイト１００では、（ｃ４）の処理として、コンテンツ管理配信サイト２００から受信した暗号化コンテンツ：Ｅｎｃ［Ｋｃ（Ｃｏｎｔｅｎｔ）］５１１を、先の（ｃ２）の処理で取得したコンテンツ鍵（Ｋｃ）５０３を用いて復号処理を実行し、コンテンツ（Ｃｏｎｔｅｎｔ）５２０を取得する。

【００９１】取得したコンテンツは、データ処理手段１１０のインタフェースを介して接続されたセットトップボックス、または再生手段としてのＴＶに転送され再生される。

【００９２】上述した処理において、コンテンツ管理配信サイト２００は、暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］５１２とメタデータ５２１の双方のデータからハッシュ(Ｈａｓｈ)値を計算して、コンテンツ管理配信サイトの秘密鍵（Ｋｓ）で署名処理を施す。ユーザサイト１００で実行する署名検証処理は、受信データである（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）に対する署名検証として実行されることになるので、署名対象データに含まれる暗号化コンテンツ鍵を他のコンテンツのものに置きかえると署名検証処理に失敗して、後続ステップの実行が許可されない。従って、コンテンツ鍵の取得、コンテンツの復号が不可能になり、不正なコンテンツの利用は排除されることになる。また、メタデータに基づいて生成される課金ログデータも、正しいコンテンツに対応するものとなり、正しい課金処理が実行される。

【００９３】［コンテンツ配信処理例２］次に、第２のコンテンツ配信処理例として、サービス管理センタからユーザサイトに対して配送鍵（Ｋｄ）を送信することなく、各ユーザに予めユーザ毎の個別鍵を渡し、コンテンツ管理配信サイトが各個別鍵で暗号化した配送鍵を暗号化コンテンツとともにユーザサイトに配信するシステム構成例について図１０を参照して説明する。

【００９４】本例のコンテンツ配信システムでは、サブ配送鍵（Ｋｄ）および個別鍵（Ｋｉ）を用いる。ただしｉ＝１～ｎであり、各々が異なる鍵である。この個別鍵（Ｋｉ）は、契約ユーザに対してサービス管理センタが例えばセキュアモジュール構造を持つＩＣカードに個別鍵（Ｋｉ）を内蔵して契約ユーザに付与または貸与する。ユーザは、個別鍵（Ｋｉ）を内蔵したＩＣカードをデータ処理手段１１０（図7.図8参照）にセットして、個別鍵（Ｋｉ）を適用した処理を実行する。例えば図８のデータ処理手段構成において、セキュアモジュール１１５がデータ処理手段１１０に対して着脱可能なＩＣカードとして構成される。

【００９５】図１０を参照して本実施例におけるコンテンツ配信処理のシーケンスを説明する。図１０には、前述の実施例１と同様、Ａ．サービス管理センタ３００における処理（ａ１）．（ａ２）、Ｂ．コンテンツ管理配信サイトにおける処理（ｂ１）～（ｂ５）、Ｃ．ユーザサイトにおける処理（ｃ１）～（ｃ４）を示している。各処理について説明する。

【００９６】まず、Ａ．サービス管理センタ３００は、個別鍵（Ｋｉ）６０１およびサブ配送鍵（ＳｕｂＫｄ）６０２を生成し、これらについての処理を実行する。個別鍵（Ｋｉ）は、契約ユーザの数に応じて契約ユーザ毎に生成するものであり、契約ユーザに対して例えばＩＣカード等のモジュールに格納して配布した後は、Ａ．サービス管理センタ３００において同一の鍵を保持管理する。また、サブ配送鍵（ＳｕｂＫｄ）は、配信コンテンツ毎に生成、あるいは定期的に更新する鍵として設定する。サービス管理センタ３００は、これらの鍵を乱数に基づいて生成する。サービス管理センタ３００は、（ａ１）の処理として、各個別鍵（Ｋｉ）６０１を用いて、サブ配送鍵（ＳｕｂＫｄ）６０２を暗号化する処理を行なう。Ａ．サービス管理センタ３００は、契約ユーザ数に応じて生成済みのｎ個の個別鍵（ｋｉ）６０１（ｉ＝１～ｎ）を適用してサブ配送鍵（ＳｕｂＫｄ）６０２を暗号化し、ｎ個の暗号化サブ配送鍵：Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］を生成する。

【００９７】暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、例えば代表的な共通鍵暗号アルゴリズムであるＤＥＳ（Data Encryption Standard）が適用できる。さらに、安全性を増すためにＤＥＳアルゴリズムを３重にして処理を行なうトリプルＤＥＳを適用してもよい。ＤＥＳ暗号化処理では鍵長５６ビットの鍵を適用し、トリプルＤＥＳでは１１２ビットの鍵長を持つ鍵を適用することになる。サービス管理センタ３００は、適用する暗号化方式に応じた鍵長の個別鍵（Ｋｉ）６０１およびサブ配送鍵（ＳｕｂＫｄ）６０２を生成する。

【００９８】（ａ１）の処理の結果、ｎ個の個別鍵（Ｋｉ）で暗号化処理されたサブ配送鍵（ＳｕｂＫｄ）、す

なわち、Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］（ｉ＝１～ｎ）が生成される。ｎ個の暗号化サブ配送鍵Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］は、コンテンツ管理配信サイト２００に転送される。

【００９９】また、サブ配送鍵（ＳｕｂＫｄ）６０２についても、コンテンツ管理配信サイト２００に転送するが、通信路におけるデータ漏洩等の問題の発生を避けるため、（ａ２）の処理として、サブ配送鍵（ＳｕｂＫｄ）６０２の暗号化処理（ＤＥＳ）を実行してコンテンツ管理配信サイト２００に転送する。この場合の暗号化鍵としては、例えばコンテンツ管理配信サイト２００と、サービス管理センタ３００間において相互認証処理を実行し、認証処理の際に生成するセッション鍵（Ｋｓ）を適用することができる。あるいは双方が共通に保有する共通鍵、またはパスワードを用いて暗号化、復号化処理を実行する構成としてもよい。

【０１００】次に、Ｂ．コンテンツ管理配信サイト２００における処理について説明する。コンテンツ管理配信サイト２００は、まず（ｂ１）の処理として、コンテンツを暗号化するためのコンテンツ鍵（Ｋｃ）６０３を生成する。コンテンツ鍵は、乱数発生装置において発生した乱数に基づいて生成するものであり、コンテンツ毎に生成する。コンテンツ鍵による暗号化処理が例えばＤＥＳ暗号化処理である場合は鍵長５６ビットの鍵を生成してコンテンツ鍵とし、トリプルＤＥＳの場合は１１２ビットの鍵長を持つ鍵をコンテンツ鍵として生成する。

【０１０１】次に、コンテンツ管理配信サイト２００は、（ｂ２）の処理として、生成したコンテンツ鍵（Ｋｃ）を用いてコンテンツの暗号化処理を実行する。暗号化処理のアルゴリズムとしては各種のアルゴリズムが適用可能であり、ＤＥＳ（Data Encryption Standard）、またはトリプルＤＥＳが適用できる。この暗号化処理の結果、暗号化コンテンツ：Ｅｎｃ［Ｋｃ（Ｃｏｎｔｅｎｔ）］６１１が生成される。

【０１０２】さらに、コンテンツ管理配信サイト２００は、（ｂ３）の処理として、サービス管理センタ３００から受信した暗号化されたサブ配送鍵データ：Ｅｎｃ［Ｋｓ（ＳｕｂＫｄ）］をセッション鍵Ｋｓで復号し、サブ配送鍵（ＳｕｂＫｄ）６０２を取得する。

【０１０３】次に、コンテンツ管理配信サイト２００は、（ｂ４）の処理として、取得したサブ配送鍵（ＳｕｂＫｄ）６０２を用いて、コンテンツ鍵（Ｋｓ）の暗号化処理を実行して暗号化コンテンツ鍵データ：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］６１２を生成する。

【０１０４】次に、コンテンツ管理配信サイト２００は、暗号化コンテンツ鍵データ：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］６１２と、価格情報、コピー制限情報等の各種のコンテンツ関連利用情報からなるメタデータ６２１との双方のデータ、すなわち、（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）からハッシュ（Ｈａｓｈ）値を計算し、コンテンツ管理配信サイト２００の秘密鍵（Ｋｓ）を用いた署名生成処理（ｂ５）を実行する。署名生成処理は、例えば楕円曲線暗号方式の署名アルゴリズムであるＥＣＣ－ＤＳＡに従って実行される。

【０１０５】コンテンツ管理配信サイト２００は、上述の処理によって生成した暗号化コンテンツ：Ｅｎｃ［Ｋｃ（Ｃｏｎｔｅｎｔ）］６１１、署名処理を施した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］６１２とメタデータ６２１、および、サービス管理センタ３００から受信した暗号化サブ配送鍵：Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］６１３、さらに、コンテンツ管理配信サイト２００の公開鍵（Ｋｐ）を格納した公開鍵証明書ををユーザサイトに向けて配信する。

【０１０６】なお、従来技術の欄で説明したＣＡＳ（Conditional Access System）において、本実施例の構成を適用することが可能であり、この場合には、コンテンツ管理配信サイト２００からユーザサイト１００に対して送信する署名処理を施した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］６１２とメタデータ６２１は、コンテンツ番組情報を含むＥＣＭ（Entitlement Control Message）内に含ませて放送データとして送信する。また、コンテンツ管理配信サイト２００からユーザサイト１００に対して送信する暗号化サブ配送鍵：Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］６１３は、各ユーザに渡されているＩＣカードの識別子（ＩＤ）を付加情報として持つＥＭＭ（Entitlement Management Message）に含ませて放送波で送信する。

【０１０７】次に、上記各データを受信するユーザサイト１００における処理について説明する。ユーザサイト１００では、通信衛星またはインターネット等の通信手段を介して例えばセットトップボックス等の受信手段１２０においてデータ受信を行ない、受信データをデータ処理手段１１０に転送する。受信データは、データ処理手段１１０の例えばハードディスク等の記憶手段に一旦格納される。

【０１０８】図１０では、これらの格納データに対する処理手順を（ｃ１）～（ｃ４）として示している。まず、ユーザサイト１００では、（ｃ１）の処理として、コンテンツ管理配信サイト２００から受信した署名処理を施した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］６１２とメタデータ６２１の署名検証処理を実行する。署名検証処理は、署名を、受信した公開鍵証明書から取り出したコンテンツ管理配信サイト２００の公開鍵を適用して解いた復号値と、受信データである（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）からハッシュ（Ｈａｓｈ）値を計算した結果とが一致するか否かによって実行される。一致していた場合は、署名が正しく、データ、すなわち、受信データである（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）の改竄がないと判定され、次の処理ステップの実行が許可される。署名検証に

おいて両データが一致しなかった場合は、データ改竄の可能性があると判定されて、次の処理が実行されず、処理は終了する。

【０１０９】署名検証に成功すると、次に、ユーザサイト１００では、（ｃ２）の処理として、コンテンツ管理配信サイト２００から受信した暗号化サブ配送鍵：Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］６１３を、サービス管理センタ３００から予め受領済みの個別鍵（Ｋｉ）６０１を用いて復号処理を実行し、サブ配送鍵（ＳｕｂＫｄ）６０２を取得する。

【０１１０】コンテンツ管理配信サイト２００から受信する暗号化サブ配送鍵：Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］６１３は、ユーザ数に応じた１～ｎの各個別鍵で暗号化したサブ配送鍵のデータである。コンテンツ管理配信サイト２００から受信する暗号化サブ配送鍵：Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］（ｉ＝１～ｎ）には各データ毎に識別データが付与されており、この識別データは、各ユーザに渡されているＩＣカードの識別子（ＩＤ）に対応するものとなっている。ユーザサイトのデータ処理手段のセキュアモジュール（ＩＣカード）では、自己のＩＣカードに一致するＩＤを持つ暗号化サブ配送鍵：Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］データの選択処理を実行して、選択された暗号化サブ配送鍵：Ｅｎｃ［Ｋｉ（ＳｕｂＫｄ）］に対して、ＩＣカードに格納された個別鍵（Ｋｉ）を適用した復号処理を実行してサブ配送鍵（ＳｕｂＫｄ）を取得する。

【０１１１】次に、ユーザサイト１００では、（ｃ３）の処理として、コンテンツ管理配信サイト２００から受信した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］６１２を、先の（ｃ１）の処理で取得したサブ配送鍵（ＳｕｂＫｄ）６０２を用いて復号処理を実行し、コンテンツ鍵（Ｋｃ）６０３を取得する。この復号処理の実行対象は、署名対象データ中に格納された暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］６１２である。

【０１１２】次に、ユーザサイト１００では、（ｃ４）の処理として、コンテンツ管理配信サイト２００から受信した暗号化コンテンツ：Ｅｎｃ［Ｋｃ（Ｃｏｎｔｅｎｔ）］６１１を、先の（ｃ２）の処理で取得したコンテンツ鍵（Ｋｃ）６０３を用いて復号処理を実行し、コンテンツ（Ｃｏｎｔｅｎｔ）６２０を取得する。

【０１１３】取得したコンテンツは、データ処理手段１１０のインタフェースを介して接続されたセットトップボックス、または再生手段としてのＴＶに転送され再生される。

【０１１４】上述した処理例においても、コンテンツ管理配信サイト２００は、暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］６１２とメタデータ６２１の双方のデータからハッシュ(Ｈａｓｈ)値を計算して、コンテンツ管理配信サイトの秘密鍵（Ｋｓ）で署名処理を施す。ユーザサイト１００で実行する署名検証処理は、受信データである（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）に対する署名検証として実行されることになるので、署名対象データに含まれる暗号化コンテンツ鍵を他のコンテンツのものに置きかえると署名検証処理に失敗して、後続ステップの実行が許可されない。従って、コンテンツ鍵の取得、コンテンツの復号が不可能になり、不正なコンテンツの利用は排除されることになる。また、メタデータに基づいて生成される課金ログデータも、正しいコンテンツに対応するものとなり、正しい課金処理が実行される。

【０１１５】個別鍵（Ｋｉ）６０１は、コンテンツ管理配信サイト２００から正規なユーザサイト１００にのみ安全なセキュアモジュール（例えばＩＣカード）に格納されて配布され、正規なユーザサイト１００において管理されることにより、漏洩は防止される。

【０１１６】このように、本発明のシステムにおいては、個別鍵（Ｋｉ）を、コンテンツの配信を行なう例えば放送局のようなコンテンツ管理配信サイトに渡すことなく、暗号化コンテンツ配信が実現され、コンテンツ管理配信サイトにおける個別鍵（Ｋｉ）の安全管理体制を強いることなく鍵の漏洩が防止され、コンテンツの保護構成が実現されることになる。

【０１１７】［メタデータおよびコンテンツ鍵に対する署名処理］図１１に、本発明の構成において実行される電子署名の検証に基づくコンテンツ（番組）再生の各種態様について説明する図を示す。

【０１１８】図１１（ａ）は、正しいコンテンツ利用態様、すなわち署名検証が成立（ＯＫ）し、コンテンツ（番組）再生が許可される場合の例である。コンテンツ管理配信サイトでは、価格情報を含むメタデータ、サブ配送鍵（ＳｕｂＫｄ）で暗号化したコンテンツ鍵に対するハッシュ（Ｈａｓｈ）値を計算し、秘密鍵（Ｋｓ）を用いて署名を生成し、ユーザサイトに送信する。なお、サブ配送鍵（ＳｕｂＫｄ）は、配送鍵（ｋｄ）または、個別鍵（Ｋｉ）によって暗号化された暗号化サブ配送鍵としてユーザサイトに送信される。

【０１１９】ユーザサイトでは、暗号化サブ配送鍵を配送鍵（ｋｄ）または、個別鍵（Ｋｉ）によって復号し、サブ配送鍵（ＳｕｂＫｄ）を取得し、コンテンツ(番組A)に対応するコンテンツ鍵（Ｋｃ－ａ）を暗号化している配送鍵（Ｋｄ）を、取得したサブ配送鍵（ＳｕｂＫｄ）で復号することにより取得して、さらに、配送鍵（Ｋｄ）に基づいて暗号化コンテンツ鍵の復号処理を実行することにより、コンテンツ鍵（Ｋｃ－ａ）を取得し、取得したコンテンツ鍵（Ｋｃ－ａ）で暗号化コンテンツの復号を行なってコンテンツを再生利用することができる。

【０１２０】しかし、図９、図１０を用いて説明したように、配送鍵（ｋｄ）または、個別鍵（Ｋｉ）によって

暗号化された暗号化サブ配送鍵の復号処理の実行条件として、署名の検証に成功することが設定されている。

【０１２１】図１１（ａ）の場合は、番組Ａに対するメタデータと番組Ａの暗号化コンテンツ鍵（Ｋｃ－ａ）に対してハッシュ値が計算されて署名がなされ、ユーザサイトは署名検証をコンテンツ管理配信サイトの公開鍵証明書から取り出した公開鍵を用いて実行する。番組Ａに対するメタデータと番組Ａの暗号化コンテンツ鍵（Ｋｃ－ａ）に基づいて計算したハッシュ値と、署名に対して公開鍵を適用した処理によって取得される値は、データの改竄、置き換えがなされていないので、一致することになる。従って、次のステップとして、配送鍵（ｋｄ）または、個別鍵（Ｋｉ）によって暗号化された暗号化サブ配送鍵の復号処理が実行され、さらに後続処理（図９，１０における（ｃ２）～（ｃ４））を実行して、コンテンツの再生が可能となる。

【０１２２】図１１（ｂ）の場合は、番組Ａに対するメタデータが改竄された場合を示している。例えば本来コンテンツ（番組Ａ）の価格が３００円と記録されていたものを１００円と改竄したとする。この場合、ユーザサイトで実行される署名検証処理は、改竄されたメタデータと番組Ａの暗号化コンテンツ鍵（Ｋｃ－ａ）に基づいて計算したハッシュ値と、署名に対して公開鍵を適用した処理によって取得される値との比較として実行される。この比較処理においては、データの一致は得られないことになる。署名は、改竄されたメタデータと異なる番組Ａの本来のメタデータと番組Ａの暗号化コンテンツ鍵（Ｋｃ－ａ）に基づいて計算したハッシュ値に対してなされたものであるからである。従って、署名検証成立を条件として実行可能となる暗号化サブ配送鍵の復号処理が実行されず、さらに後続処理（図９．１０における（ｃ２）～（ｃ４））も実行不可能となり、コンテンツの再生が不可能となる。

【０１２３】図１１（ｃ）の場合は、番組Ａに対するメタデータと番組Ａの暗号化コンテンツ鍵（Ｋｃ－ａ）に対する署名検証を実行し、署名検証の成立に基づいて、他のコンテンツ（番組Ｂ）の利用を行なおうとする例である。すなわち、メタデータと署名との置き換え処理によって他のコンテンツの不正利用を実行しようとした場合の処理例である。この場合、ユーザサイトで実行される署名検証処理は、番組Ａのメタデータと番組Ａの暗号化コンテンツ鍵（Ｋｃ－ａ）に基づいて計算したハッシュ値と、署名に対して公開鍵を適用した処理によって取得される値との比較として実行され、この比較処理においてデータの一致が得られる。従って、次のステップとして、配送鍵（ｋｄ）または、個別鍵（Ｋｉ）によって暗号化された暗号化サブ配送鍵の復号処理が実行される。しかし、取得したサブ配送鍵によって復号取得可能なコンテンツ鍵は、署名検証に成功した番組Ａに対するコンテンツ鍵（Ｋｃ－ａ）であり、他のコンテンツ（例えば番組Ｂ）のコンテンツ鍵ではない。署名検証成立を条件として取得されるコンテンツ鍵は、署名対象データに含まれるコンテンツ鍵であり、他のコンテンツの復号は防止され、コンテンツの不正利用が排除される。

【０１２４】図１２に、本発明の署名検証処理を条件とするコンテンツ利用処理について説明する図を示す。コンテンツ管理配信サイトでは、価格情報を含むメタデータ、サブ配送鍵（ＳｕｂＫｄ）で暗号化したコンテンツ鍵に対するハッシュ（Ｈａｓｈ）値を計算し、秘密鍵（Ｋｓ）を用いて署名を生成し、ユーザサイトに送信する。なお、サブ配送鍵（ＳｕｂＫｄ）は、配送鍵（ｋｄ）または、個別鍵（Ｋｉ）によって暗号化された暗号化サブ配送鍵としてユーザサイトに送信する。

【０１２５】ユーザサイトは署名検証をコンテンツ管理配信サイトの公開鍵証明書から取り出した公開鍵を用いて実行する。具体的には、番組Ａに対するメタデータと番組Ａの暗号化コンテンツ鍵（Ｋｃ－ａ）に基づいて計算したハッシュ値と、署名に対して公開鍵を適用した処理によって取得される値との比較処理を行なう。署名対象データの改竄、置き換えがなされていない場合は、一致することになる。一致したことを条件として、次のステップの実行が許可される。すなわち、配送鍵（ｋｄ）または、個別鍵（Ｋｉ）によって暗号化された暗号化サブ配送鍵の復号処理が実行され、さらに後続処理、コンテンツ(番組Ａ)に対応するコンテンツ鍵（Ｋｃ－ａ）を暗号化している配送鍵（Ｋｄ）を、取得したサブ配送鍵（ＳｕｂＫｄ）で復号することにより取得して、さらに、配送鍵（Ｋｄ）に基づいて暗号化コンテンツ鍵の復号処理を実行することにより、コンテンツ鍵（Ｋｃ－ａ）を取得し、取得したコンテンツ鍵（Ｋｃ－ａ）で暗号化コンテンツの復号を行なってコンテンツを再生利用することができる。この一連の処理で取得されるコンテンツ鍵は、署名対象データ無いに格納されたコンテンツ鍵に限られ、他のコンテンツ（番組Ｂ）の復号に適用することはできない。

【０１２６】次に、本発明のコンテンツ配信システムにおける処理手順について図１３に示すフローを用いて説明する。まず、ステップＳ３０１において、コンテンツ管理配信サイトは、コンテンツを暗号化するためのコンテンツ鍵（Ｋｃ）を、例えば乱数発生装置において発生した乱数に基づいて生成し、コンテンツ鍵によるコンテンツ（番組）の暗号化処理を実行する。暗号化処理が例えばＤＥＳ暗号化処理である場合は鍵長５６ビットのコンテンツ鍵とし、トリプルＤＥＳの場合は１１２ビットの鍵長を持つ鍵をコンテンツ鍵を適用する。

【０１２７】次に、ステップＳ３０２において、コンテンツ管理配信サイトは、サブ配送鍵（ＳｕｂＫｄ）を用いて、コンテンツ鍵（Ｋｓ）の暗号化処理を実行して暗号化コンテンツ鍵データ：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］を生成する。

【０１２８】次に、ステップＳ３０３において、コンテンツ管理配信サイトは、暗号化コンテンツ鍵データと、価格情報、コピー制限情報等の各種のコンテンツ関連利用情報からなるメタデータとの双方のデータ、すなわち、（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）からハッシュ（Ｈａｓｈ）値を計算し、コンテンツ管理配信サイトの秘密鍵（Ｋｓ）を用いた署名生成処理を実行する。署名生成処理は、例えば楕円曲線暗号方式の署名アルゴリズムであるＥＣＣ－ＤＳＡに従って実行される。

【０１２９】コンテンツ管理配信サイトは、ステップＳ３０４で、生成した暗号化コンテンツ：Ｅｎｃ［Ｋｃ（Ｃｏｎｔｅｎｔ）］、署名処理を施した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］とメタデータをユーザサイトに向けて配信する。なお、必要であればコンテンツ管理配信サイトの公開鍵証明書も併せて送付する。、

【０１３０】以下のステップＳ３０５以下の処理はユーザサイトにおける処理である。なお、ステップＳ３２１は、署名対象データであるメタデータ＋暗号化コンテンツ鍵の改竄を実行した場合（図１１（ｂ）に相当）、ステップＳ３２２は、署名対象データであるメタデータ＋暗号化コンテンツ鍵の置き換えを実行した場合（図１１（ｃ）に相当）を示している。

【０１３１】ユーザサイトでは、コンテンツ管理配信サイトから受信した署名処理を施した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］とメタデータの署名検証処理を実行する。まず、ステップＳ３０５において、受信データである（Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］＋メタデータ）からハッシュ（Ｈａｓｈ）値を計算する」この取得値を①とする。次にステップＳ３０６において、受信した署名を、コンテンツ管理配信サイトの公開鍵を適用して解き、値を取得する。この取得値を②とする。

【０１３２】ステップＳ３０７では、上記取得値①、②の比較を実行する。一致していない場合は、署名検証に失敗と判定され、以下の処理は実行されず、処理は終了する。ステップＳ３２１におけるデータ改竄、ステップＳ３０７において不一致（ｆａｌｓｅ）となり、処理が終了となり、コンテンツは再生されない。

【０１３３】ステップＳ３０７で署名検証に成功（ｔｒｕｅ）した場合は、ステップＳ３０８に進み、コンテンツ管理配信サイトから受信した暗号化サブ配送鍵：Ｅｎｃ［Ｋｄ（ＳｕｂＫｄ）］を、配送鍵（Ｋｄ）または個別鍵（Ｋｉ）を用いて復号し、サブ配送鍵（ＳｕｂＫｄ）を取得する。

【０１３４】次に、ステップＳ３０９では、コンテンツ管理配信サイトから受信した暗号化コンテンツ鍵：Ｅｎｃ［ＳｕｂＫｄ（Ｋｃ）］を、先の処理で取得したサブ配送鍵（ＳｕｂＫｄ）を用いて復号し、コンテンツ鍵（Ｋｃ）を取得する。

【０１３５】次に、ステップＳ３１０において、取得したコンテンツ鍵（Ｋｃ）が再生対象コンテンツ(番組)のコンテンツ鍵として適用できるか否かを判定する。正当なデータに対して署名検証処理が実行されていれば、取得したコンテンツ鍵（Ｋｃ）は、再生対象コンテンツ(番組)のコンテンツ鍵として適用できる。しかし、ステップＳ３２２におけるデータ置き換えが行われた場合は、署名検証の結果後の一連の処理によって取得されるコンテンツ鍵（Ｋｃ）は、再生対象コンテンツ(番組)のコンテンツ鍵として適用できない。従って、コノ時点で処理は終了する。

【０１３６】取得したコンテンツ鍵（Ｋｃ）が、再生対象コンテンツ(番組)のコンテンツ鍵である場合は、ステップＳ３１１において、コンテンツ管理配信サイトから受信した暗号化コンテンツ：Ｅｎｃ［Ｋｃ（Ｃｏｎｔｅｎｔ）］を、取得したコンテンツ鍵（Ｋｃ）を用いて復号し、コンテンツ（Ｃｏｎｔｅｎｔ）を取得し、ステップＳ３１２において、コンテンツ（番組）を再生する。さらに、ステップＳ３１３において、署名検証処理の対象データ中に含まれるメタデータに記録された価格情報に基づいて課金情報を生成し、サービス管理センターに送信する。

【０１３７】［各エンティテイの構成］次に、上述したコンテンツ配信システムを構成する各エンティテイ、すなわち、サービス管理センタおよびコンテンツ管理配信サイトの構成例について図１４を参照して説明する。

【０１３８】サービス管理センタおよびコンテンツ管理配信サイトは他エンティテイと通信可能な通信手段を備えたデータ処理手段によって実現することができる。図１４にシステム構成例を示す。なお、図１４に示すシステム構成例は１つの例であり、各システムは、ここに示すべての機能を必ずしも備えることが要求されるものではない。図１４に示すＣＰＵ(Central processing Unit)７０１は、各種アプリケーションプログラムや、ＯＳ（Operating System）を実行するプロセッサである。ＲＯＭ（Read-Only-Memory）７０２は、ＣＰＵ７０１が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。ＲＡＭ（Random Access Memory）７０３は、ＣＰＵ７０１の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【０１３９】ＨＤＤ７０４はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。暗号処理手段７０５は、送信データの暗号処理、復号処理、署名生成、検証処理等を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをＲＯＭ７０２に格納し、ＣＰＵ７０１がＲ

OM格納プログラムを読み出して実行するように構成してもよい。メモリ（セキュアモジュール）７０６は例えば耐タンパ構造を持つメモリとして構成され、暗号処理に必要な鍵データ、アクセス許可書の格納領域として使用可能である。なお、これらのデータは、他のメモリ領域、記憶媒体に格納することも可能である。

【０１４０】バス７２１はＰＣＩ（Peripheral Components Interconnect）バス等により構成され、各モジュール、入出力インタフェース７２２を介した各入手力装置とのデータ転送を可能にしている。

【０１４１】入力部７１１は、例えばキーボード、ポインティングデバイス等によって構成され、ＣＰＵ７０１に各種のコマンド、データを入力するためにユーザにより操作される。出力部７１２は、例えばＣＲＴ、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。

【０１４２】通信部７１３はデバイスの接続したエンティティ、例えばサービス管理センタまたはコンテンツ管理配信サイト、またはユーザサイト等との通信処理を実行し、ＣＰＵ７０１の制御の下に、各記憶部から供給されたデータ、あるいはＣＰＵ７０１によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティティからのデータを受信する処理を実行する。

【０１４３】ドライブ７１４は、フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体７１５の記録再生を実行するドライブであり、各リムーバブル記録媒体７１５からのプログラムまたはデータ再生、リムーバブル記録媒体７１５に対するプログラムまたはデータ格納を実行する。

【０１４４】各記憶媒体に記録されたプログラムまたはデータを読み出してＣＰＵ７０１において実行または処理を行なう場合は、読み出したプログラム、データは入出力インタフェース７２２、バス７２１を介して例えば接続されているＲＡＭ７０３に供給される。

【０１４５】先の説明内に含まれるサービス管理センタ、コンテンツ管理配信サイトにおける処理を実行するためのプログラムは例えばＲＯＭ７０２に格納されてＣＰＵ７０１によって処理されるか、あるいはハードディスクに格納されＨＤＤ７０４を介してＣＰＵ７０１に供給されて実行される。

【０１４６】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１４７】なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０１４８】例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read OnlyMemory)に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１４９】なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０１５０】なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

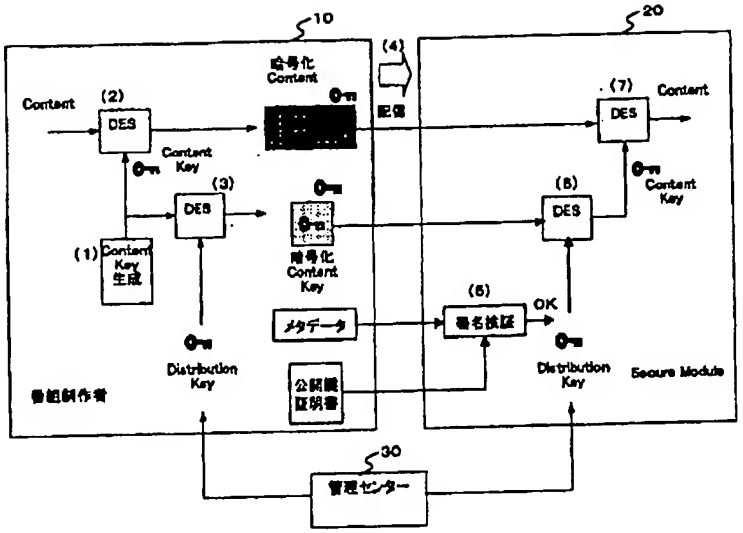
【０１５１】

【発明の効果】以上、説明したように、本発明のコンテンツ配信システム、コンテンツ配信方法、およびデータ処理装置、データ処理方法、並びにコンピュータ・プログラムによれば、暗号化コンテンツの配信を行ない、正規ユーザにおいてのみコンテンツの利用を許容しようとするシステムにおいて、コンテンツの配信を行なう例えば放送局のようなコンテンツ管理配信サイトにおいて、コンテンツの価格情報を含むメタデータと、コンテンツの暗号処理に適用するコンテンツ鍵を併せたデータのハッシュ値を生成して電子署名を実行し、データを受信したユーザサイトにおいて、署名検証の成立を条件として署名対象データ中に格納されたコンテンツ鍵の取得を可能とする構成としたので、メタデータの改竄、あるいはメタデータを含むデータの置き換えなどの不正な処理によるコンテンツの不正利用を防止することが可能となる。

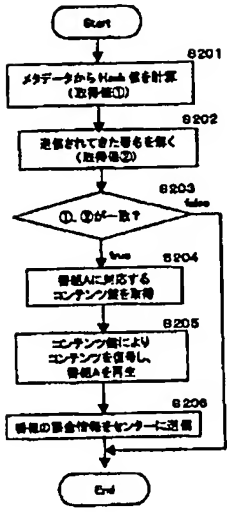
【図面の簡単な説明】

【図１】従来のコンテンツ配信システムの処理構成を説明する図である。
【図２】従来のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明する図である。
【図３】従来のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明する図である。
【図４】従来のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明する図である。
【図５】従来のコンテンツ配信システムにおけるメタデータの置き換えによるコンテンツ不正利用について説明するフロー図である。
【図６】従来のコンテンツ配信システムにおける署名検証に基づくコンテンツ利用について説明するフロー図である。
【図７】本発明のコンテンツ配信システムの概要を説明するブロック図である。
【図８】本発明のコンテンツ配信システムのユーザサイトに構成されるデータ処理装置の構成例を示すブロック図である。
【図９】本発明のコンテンツ配信システムのコンテンツ配信処理例（実施例１）を示す図である。
【図１０】本発明のコンテンツ配信システムのコンテンツ配信処理例（実施例２）を示す図である。
【図１１】本発明のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明する図である。
【図１２】本発明のコンテンツ配信システムにおける署名検証に基づくコンテンツ利用について説明する図である。
【図１３】本発明のコンテンツ配信システムにおける署名生成、検証に基づくコンテンツ利用について説明するフロー図である。
【図１４】本発明のコンテンツ配信システムのサービス管理センタ、コンテンツ管理配信サイトのシステム構成例を示す図である。
【符号の説明】
１０　コンテンツ提供サイト
２０　ユーザサイト
３０　管理センター
１００　ユーザサイト
１１０　データ処理手段
１１５　セキュアモジュール
１２０　受信手段
１４０　出力手段
２００　コンテンツ管理配信サイト
２２０　コンテンツ管理部
２３０　コンテンツ配信部
３００　サービス管理センタ
４００　認証局
１０１　ＣＰＵ(Central processing Unit)
１０２　ＲＯＭ (Read-Only-Memory)
１０３　ＲＡＭ (Random Access Memory)
１０４　ＨＤＤ
１０５，１０６　通信Ｉ／Ｆ
１２１　制御部
１２２　暗号／復号化部
１２３　内部メモリ
５０１　配送鍵
５０２　サブ配送鍵
５０３　コンテンツ鍵
５１１　暗号化コンテンツ
５１２　暗号化コンテンツ鍵
５１３　暗号化サブ配送鍵
５２０　コンテンツ
５２１　メタデータ
５２２　公開鍵証明書
６０１　個別鍵
６０２　サブ配送鍵
６０３　コンテンツ鍵
６１１　暗号化コンテンツ
６１２　暗号化コンテンツ鍵
６１３　暗号化サブ配送鍵
６２０　コンテンツ
６２１　メタデータ
６２２　公開鍵証明書
７０１　ＣＰＵ(Central processing Unit)
７０２　ＲＯＭ (Read-Only-Memory)
７０３　ＲＡＭ (Random Access Memory)
７０４　ＨＤＤ
７０５　暗号処理手段
７０６　メモリ（セキュアモジュール）
７１１　入力部
７１２　出力部
７１３　通信部
７１４　ドライブ
７１５　リムーバブル記録媒体
７２１　バス
７２２　入出力インタフェース

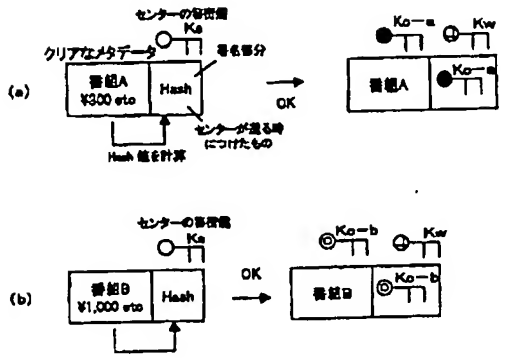
【図１】


10
20
30
(1)
(2)
(3)
(4)
(5)
(6)
(7)
Content
DES
Content Key
Content Key 生成
暗号化 Content
配信
暗号化 Content Key
メタデータ
署名検証
OK
Distribution Key
公開鍵証明書
番組制作者
Secure Module
管理センター

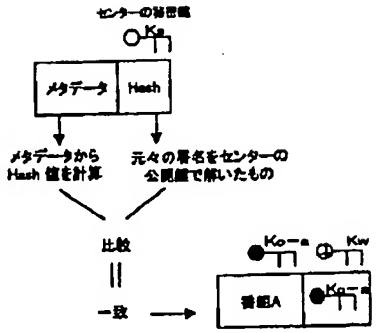
【図６】


Start
S201
メタデータからHash値を計算
S202
送信されてきた署名を開く
S203
false
true
S204
番組Aに対応する
コンテンツ鍵を取得
S205
コンテンツ鍵により
コンテンツを復号し、
番組Aを再生
S206
End

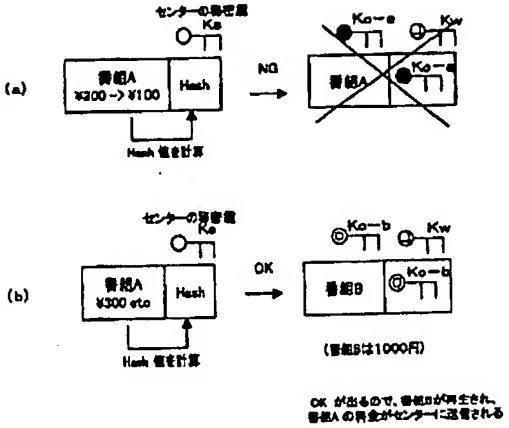
【図２】


センターの秘密鍵
Ks
クリアなメタデータ
署名部分
(a)
番組A
¥300 etc
Hash
センターが送る時につけたもの
Hash 値を計算
OK
Ko−a
Kw
番組A
(b)
番組B
¥1,000 etc
Ko−b
番組B

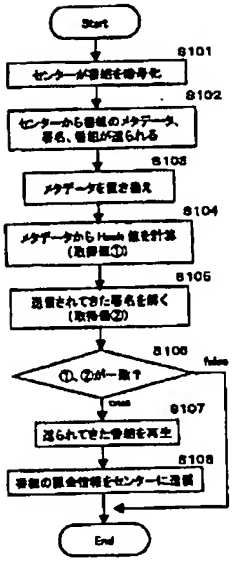
【図４】


センターの秘密鍵
Ks
メタデータ
Hash
メタデータから
Hash 値を計算
元々の署名をセンターの
公開鍵で解いたもの
比較
一致
Ko−a
Kw
番組A

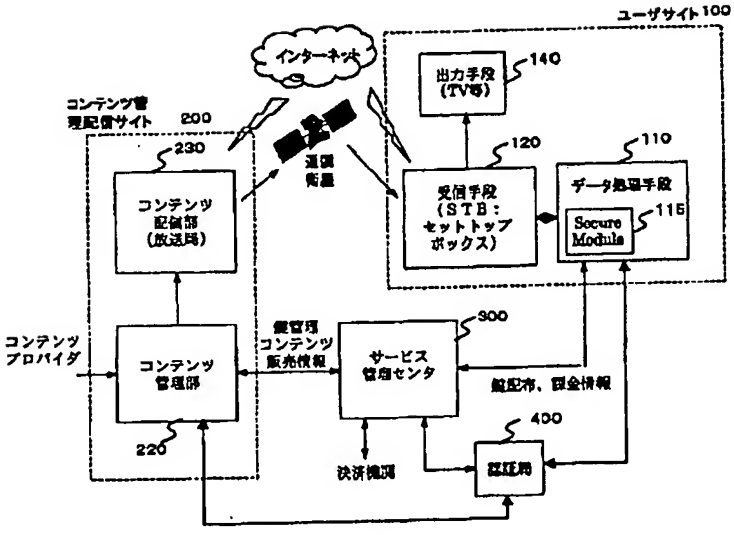
【図3】


センターの暗号鍵
Ke
(a)
番組A
¥300 -> ¥100
Hash
Hash 値を計算
NG
Ko-a
Kw
番組A
Ko-a
(b)
番組A
¥300 etc
Hash
Hash 値を計算
OK
Ko-b
Kw
番組B
Ko-b
(番組Bは1000円)
OK が出るので、番組Bが再生され、
番組Aの料金がセンターに送信される

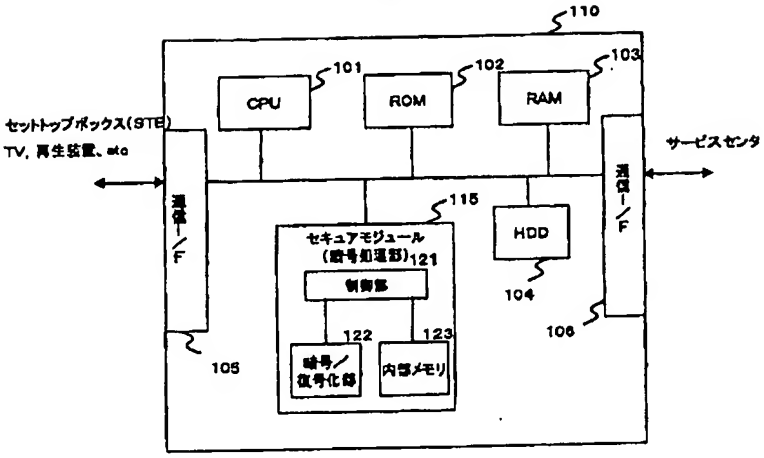
【図5】


Start
S101
センターが番組を暗号化
S102
センターから番組のメタデータ、
署名、番組が送られる
S103
メタデータを置き換え
S104
メタデータからHash 値を計算
(取得値①)
S105
送信されてきた署名を解く
(取得値②)
S106
①、②が一致？
false
true
S107
送られてきた番組を再生
S108
番組の課金情報をセンターに送信
End

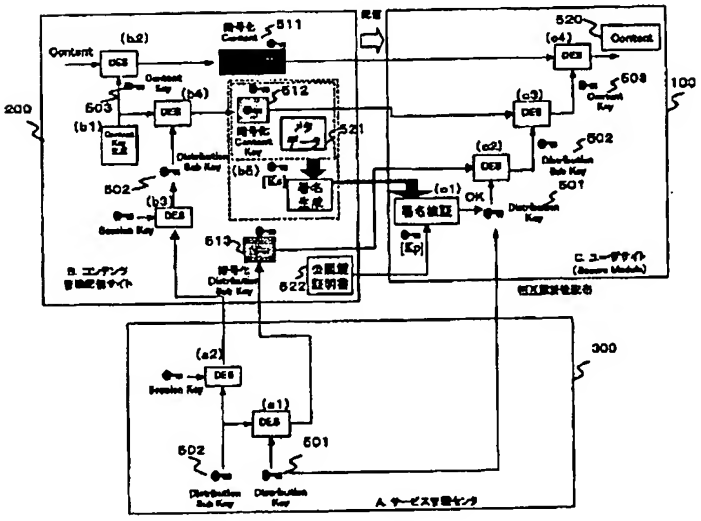
【図7】


ユーザサイト100
インターネット
出力手段
(TV等)
140
コンテンツ管
理配信サイト
200
230
通信
衛星
120
110
コンテンツ
配信部
(放送局)
受信手段
(STB:
セットトップ
ボックス)
データ処理手段
Secure
Module
115
コンテンツ
プロバイダ
コンテンツ
管理部
220
鍵管理
コンテンツ
販売情報
サービス
管理センタ
300
鍵配布、課金情報
決済機関
400
認証局

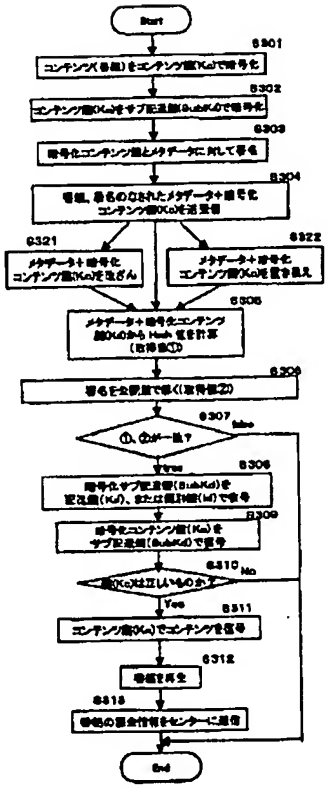
【図８】


110
CPU
101
ROM
102
RAM
103
セットトップボックス(STB)
TV, 再生装置、etc
サービスセンタ
通信I/F
115
セキュアモジュール
(暗号処理部)121
制御部
122
123
暗号/復号化部
内部メモリ
HDD
104
106
105

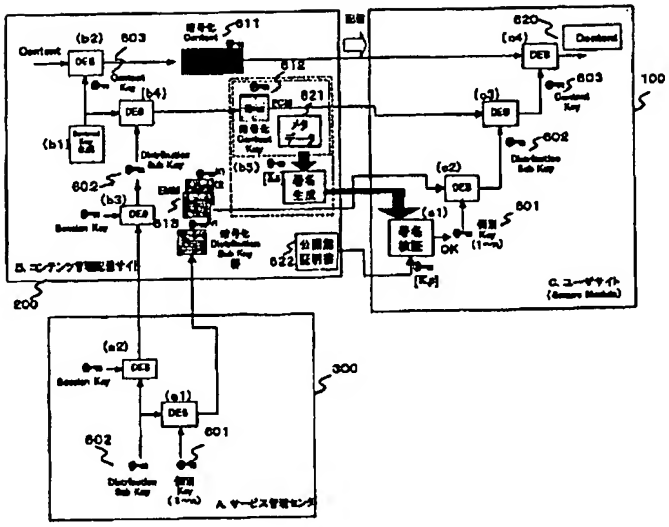
【図９】


200
100
300
Content
511
520
Content
512
521
503
508
502
501
513
522
A. サービス管理センタ
B. コンテンツ
C. ユーザサイト

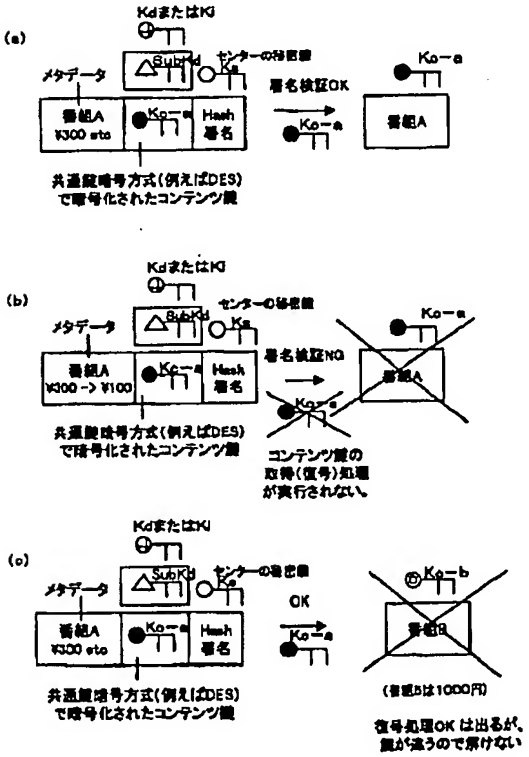
【図１３】


Start
S301
S302
S303
S304
S321
S322
S306
S309
S310
S311
S312
End

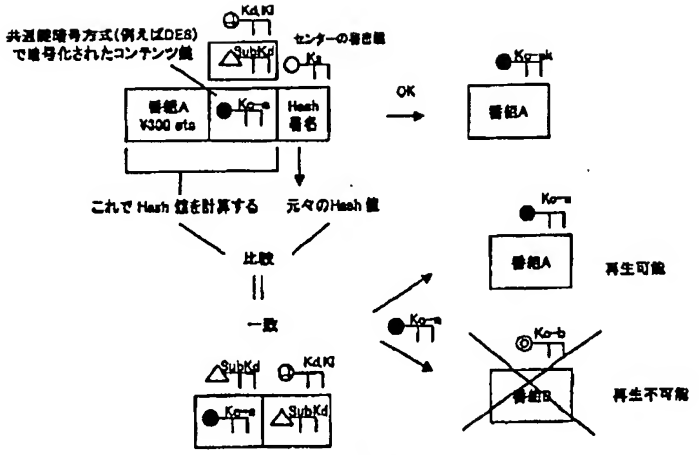
【図１０】



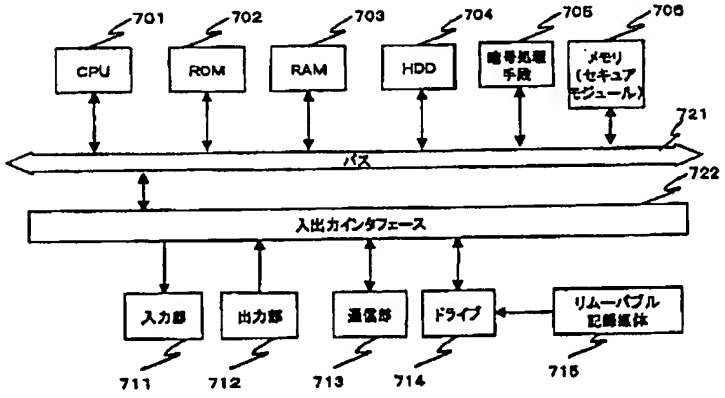
【図１１】


(a)
KdまたはKi
メタデータ
SubKd
センターの秘密鍵
Ka
番組A
¥300 etc
Ko－a
Hash
署名
署名検証OK
Ko－a
Ko－a
番組A
共通鍵暗号方式(例えばDES)
で暗号化されたコンテンツ鍵
(b)
KdまたはKi
メタデータ
SubKd
センターの秘密鍵
Ka
番組A
¥300 -> ¥100
Ko－a
Hash
署名
署名検証NG
Ko－a
Ko－a
番組A
共通鍵暗号方式(例えばDES)
で暗号化されたコンテンツ鍵
コンテンツ鍵の
取得(復号)処理
が実行されない。
(c)
KdまたはKi
メタデータ
SubKd
センターの秘密鍵
Ka
番組A
¥300 etc
Ko－a
Hash
署名
OK
Ko－a
Ko－b
番組B
(番組Bは1000円)
共通鍵暗号方式(例えばDES)
で暗号化されたコンテンツ鍵
復号処理OKは出るが、
鍵が違うので開けない

【図１２】



【図１４】



フロントページの続き

(51) Int.Cl.[7]		識別記号	F I		テーマコード（参考）
H04N	7/081		H04L	9/00	601A
	7/16				601E
// H04N	7/167		H04N	7/08	Z
				7/167	Z

Fターム(参考) 5C063 AB03 AB07 AC01 AC05 AC10
CA23 CA36 DA07 DA13 DB10
5C064 BA01 BB01 BB02 BC04 BC06
BC17 BC18 BC22 BC23 BD02
BD04 BD08 BD09 CA14 CB01
CC01 CC04
5J104 AA09 AA12 AA16 EA06 EA19
LA06 NA02 NA12 PA11